

BUNDESREPUBLIK DEUTSCHLAND

09/914109



REC'D 13 APR 2000	
WIPO	PCT

DE 00/492
EU

Bescheinigung

Die Siemens Aktiengesellschaft in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Benutzeridentifikationsverfahren"

am 23. Februar 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 07 G, G 06 F und H 04 M der Internationalen Patentklassifikation erhalten.

München, den 5. April 2000

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Joost

Aktenzeichen: 199 07 754.1



**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

This Page Blank (uspto)



Beschreibung

Benutzeridentifikationsverfahren

- 5 Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Benutzeridentifikation zur eindeutigen Identifikation eines Benutzers oder Teilnehmers eines Systems.

10 Ein solches System kann beispielsweise ein Endgerät wie ein Mobiltelefon sein oder ein Gebäude, zu dem nur bestimmte Personen Zutritt haben sollen. Es kann sich jedoch auch um ein Computernetz handeln, das den Zugriff auf bestimmte Daten nur nach eindeutiger Identifikation des Benutzers zuläßt, etwa beim Online-Banking.

15 Es ist bekannt, daß sich der Benutzer durch eine im Idealfall nur ihm bekannte persönliche Identifikationsnummer (PIN) identifiziert. Dieses Verfahren hat jedoch den Nachteil, daß der Benutzer die Nummer leicht vergessen oder aufgrund der
20 Vielzahl der zu benutzenden Nummern verwechseln kann. Daher wird die PIN-Nummer häufig in Notizbüchern oder dergleichen notiert, was jedoch ein Sicherheitsrisiko birgt.

5 Daher sind in letzter Zeit biometrische Identifikationsverfahren entwickelt worden, bei denen biometrische Merkmale eines Benutzers zur Authentifikation verwendet werden. Eine derartige biometrische Identifikation ist eine nicht einfache, aber komfortable und oft sehr sichere Methode, die Zuordnung und den Zugang einer bestimmten Person zu einem System oder einem Ort zu gewährleisten. Dabei weist die biometrische Identifikation gegenüber dem PIN-Code den Vorteil
30 auf, daß sie nicht vergessen werden kann und die biometrischen Merkmale nur sehr aufwendig oder überhaupt nicht kopierbar sind. Denn während der PIN-Code reine Software ist,
35 gibt es bei biometrischen Merkmalen immer eine mehr oder weniger eindeutige Zuordnung zur Hardware, d. h. zum Körper des jeweiligen Benutzers. Eine Möglichkeit einer derartigen bio-

metrischen Identifikation besteht in der Erfassung des Fingerabdrucks eines Fingers des Benutzers. Dieser legt beispielsweise den rechten Daumen auf eine Auflagefläche einer Eingabeeinrichtung, wo die Fingerabdrucksstrukturen mit einer Auflösung von ca. 50 μm erfaßt werden. Eine Recheneinheit vergleicht die erfaßten Fingerabdrucksmerkmale wie Verzweigungen oder Minuskeln mit den Merkmalen gespeicherter Fingerabdrücke von zugangsberechtigten Personen. Liegt ein gewisses Maß an Übereinstimmung vor, welches eine eindeutige Identifikation des Benutzers mit sehr hoher Wahrscheinlichkeit zuläßt, wird die Benutzung freigegeben.

Bei derartigen Fingerabdruckerkennungssystemen besteht jedoch das Problem, daß der Finger, insbesondere wenn er Verschmutzungen aufweist, auf dem Sensor Spuren in Form des Fingerabdrucks hinterläßt, die unter bestimmten Voraussetzungen bei einer erneuten Zugangsberechtigungsprüfung zu einer Erkennung der gleichen, berechtigten Person führen können, ohne daß der Finger erneut aufgelegt wird. Es ist beispielsweise denkbar, daß mittels eines Handschuhs oder dergleichen Druck auf den Fingerabdrucksensor mit den Spuren des Fingers des vorangehenden berechtigten Benutzers ausgeübt wird und so der berechnete Benutzer erneut erkannt wird. Daraus können sich Mißbrauchsmöglichkeiten der Benutzeridentifikation ergeben.

Der Erfindung liegt daher das Problem zugrunde, ein Verfahren zur Benutzeridentifikation mittels biometrischer Daten, insbesondere Fingerabdrucksdaten, vorzuschlagen, bei dem eine fälschliche Identifikation aufgrund von zurückgebliebenen Spuren eines vorangehenden Identifikationsvorgangs vermieden wird.

Gelöst wird die Aufgabe durch ein Identifikationsverfahren aufweisend die Schritte

(I) Erfassung eines biometrischen Datensatzes des Benutzers und der jeweiligen räumlichen Position der biometrischen Daten relativ zu einer Referenzposition,

(II) Speicherung des biometrischen Datensatzes und der zugehörigen Positionsdaten,

(III) Auslesen des biometrischen Datensatzes und der zugehörigen Positionsdaten eines dem aktuellen Identifikationsvorgangs vorangehenden Identifikationsvorgangs,

(IV) Vergleich der aktuell erfaßten biometrischen Daten und zugehörigen Positionsdaten mit den ausgelesenen vorhergehenden biometrischen Daten und zugehörigen Positionsdaten und Ablehnung der Identifikation dann, wenn die biometrischen Daten ein festgelegtes Maß an Übereinstimmung aufweisen und die Position der übereinstimmenden biometrischen Daten innerhalb eines festgelegten Toleranzbereiches übereinstimmt.

Die Erfindung geht davon aus, daß es einem Benutzer in der Regel nicht gelingt, den Finger beim erneuten Auflegen auf den Sensor mit einer Genauigkeit von weniger als 100 µm in Vertikal- und Horizontalrichtung zu positionieren. Wird bei zwei aufeinanderfolgenden Identifikationsvorgängen ein übereinstimmender Fingerabdruck in übereinstimmender Position erfaßt, so wird davon ausgegangen, daß beim zweiten Identifikationsvorgang lediglich die vom vorangehenden Identifikationsvorgang verbleibenden Abdrucksspuren mißbräuchlich verwendet werden und die Zugangsberechtigung verweigert.

Die Erfindung schlägt auch eine Vorrichtung zur biometrischen Benutzeridentifikation mit den Merkmalen des Anspruchs 8 vor. Vorteilhafte Weiterbildungen des erfindungsgemäßen Verfahrens und der erfindungsgemäßen Vorrichtung sind in den Unteransprüchen beschrieben.

Bei einer vorteilhaften Weiterbildung des Verfahrens wird bei der Erfassung des biometrischen Datensatzes ein Mittelwert der Positionen mehrerer Einzelmerkmale der biometrischen Daten ermittelt und bei der Positionsvergleichsprüfung zweier aufeinanderfolgender Identifikationsvorgänge diese Positionsmittelwerte miteinander verglichen. Da die Mittelwerte einer geringerer Streuung etwa aufgrund von einer Dehnung oder

Stauchung der Hautoberfläche oder wegen des Erfassungsrasters der Aufnahmevorrichtung unterliegen, kann bei dieser Verfahrensvariante der Toleranzbereich, innerhalb dessen eine Positionsübereinstimmung als Mißbrauch bewertet wird, enger gewählt werden, so daß eine unerwünschte Nichterkennung eines korrekt zweimal hintereinander aufgelegten Fingers unwahrscheinlicher wird.

Die Erfindung wird im folgenden anhand von Ausführungsbeispielen unter Bezugnahme auf die Zeichnungen im Detail erläutert, in denen

Fig. 1 ein schematisches Blockschaltbild eines Ausführungsbeispiels der erfindungsgemäßen Vorrichtung zeigt,
Fig. 2 ein Flußdiagramm zur Erläuterung eines Ausführungsbeispiels des erfindungsgemäßen Verfahrens zeigt, und
Fig. 3 ein Flußdiagramm zur Erläuterung eines weiteren Ausführungsbeispiels des erfindungsgemäßen Verfahrens zeigt.

Ein Ausführungsbeispiel der Erfindung wird zunächst anhand des Blockschaltbilds von Fig. 1 erläutert.

Ein Fingerabdrucksensor 1 weist ein Auflagefeld 5 zur Auflage eines Fingers (gestrichelt angedeutet) auf und erfaßt die Merkmale wie Verzweigungen oder Minuskeln des Fingerabdrucks.
Eine Positionserfassungseinrichtung 2 erfaßt die Positionen dieser Merkmale relativ zu einer Referenzposition, beispielsweise eines Koordinatenursprungs eines xy-Koordinatensystems des Auflagefeldes 5. Die so ermittelten Fingerabdrucksdaten und zugehörige Positionsinformation wird einem Speicher 3 und einer Vergleichseinrichtung 4 zugeführt. Aus dem Speicher 3 werden die entsprechenden Fingerabdrucksdaten und Positionsdaten der vorangehenden Fingerabdruckserfassung ausgelesen und ebenfalls der Vergleichseinrichtung 4 zugeführt. Dort werden die Fingerabdrucksmerkmale und deren Positionen verglichen und bei einer Übereinstimmung, die innerhalb eines Toleranzbereiches liegt, bewertet die Vergleichseinrichtung 4 die aktuelle Fingerabdruckserfassung bzw. den aktuellen Identifikationsmerkmalen.

tifikationsvorgang als mißbräuchliche Verwendung von Fingerabdrucksspuren des letzten Identifikationsvorgangs und lehnt den Zugang ab, was auf einer Anzeigeeinrichtung 6 angezeigt wird.

5

Die Erfindung geht dabei davon aus, daß

(1) alte Fingerabdrucksspuren beim Neuauflegen eines beliebigen Fingers keine Rolle mehr spielen und durch den Neuabdruck ersetzt werden und

10

(2) daß es einem Benutzer nicht gelingt, den Finger beim Wiederauflegen so genau zu positionieren, daß der Finger in Position und Richtung bis auf 100 µm oder 50 µm mit dem vorangehenden Fingerabdruck übereinstimmt.

15

Da die Position der verbleibenden Spuren des früheren Fingerabdrucks des vorangehenden Identifikationsvorgangs sich räumlich zum Sensor nicht verschieben kann, werden bei der vorliegenden Erfindung nicht nur die einzelnen Merkmale des Fingerabdrucks wie Verzweigungen oder Minuskeln, sondern auch deren genaue Position auf dem Auflagefeld, beispielsweise als xy-Koordinaten oder als Polarkoordinaten abgespeichert. Befinden sich bei einem erneuten Fingerabdruck eines erneuten Identifikationsvorgangs übereinstimmende Merkmale innerhalb eines Toleranzbereichs von 50 µm oder 100 µm an der gleichen räumlichen Position, so ist es sehr wahrscheinlich, daß es sich nicht um eine Neuauflage eines Fingers der gleichen Person, sondern um die Merkmale des letzten Abdrucks handelt. In diesem Fall ist die Zugangsberechtigung oder Identifikation abzulehnen und der Benutzer zur erneuten Auflage des Fingers

30

aufzufordern.

Ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens wird nun anhand des Flußdiagramms von Fig. 2 erläutert.

35

In einem Schritt S1 werden die biometrischen Daten und ihre zugehörigen Positionen auf der Auflagefläche erfaßt. Diese werden in einem Schritt S2 zur Verwendung bei dem nächstfol-

genden Benutzeridentifikationsvorgang abgespeichert. Entsprechend werden in Schritt 3 die biometrischen Daten und zugehörigen Positionen des vorangehenden Identifikationsvorgangs ausgelesen. In Schritt S4 wird verglichen, ob die Merkmale und Positionen der beiden aufeinanderfolgenden Erfassungen, d. h. der Fingerabdruckserfassung des aktuellen Benutzeridentifikationsvorgangs und der Fingerabdruckserfassung des direkt vorangehenden Benutzeridentifikationsvorgangs übereinstimmen. Wenn sowohl die Merkmale des Fingerabdruckes ein festgelegtes Maß an Übereinstimmung aufweisen als auch die Positionen dieser Merkmale innerhalb eines Toleranzbereiches von 50 μm oder 100 μm übereinstimmen, wird die Identifikation abgelehnt (Schritt S5), andernfalls geht die Prüfung weiter zu Schritt S6, in dem wie bei bekannten Benutzeridentifikationsverfahren geprüft wird, ob die Merkmale der aktuellen Erfassung des Fingerabdrucks mit den gespeicherten Merkmalen von Fingerabdrücken bestimmter Personen, beispielsweise berechtigter Benutzer, übereinstimmen. Ist dies nicht der Fall, wird die Identifikation abgelehnt (Schritt S7), andernfalls erfolgt die Identifikation.

Die in Fig. 3 erläuterte Verfahrensvariante unterscheidet sich von der in Fig. 2 dargestellten dadurch, daß in einem Schritt S11 ein Mittelwert der Positionen von erfaßten Merkmalen des biometrischen Datensatzes (Fingerabdrucks) berechnet und abgespeichert wird. In Schritt S4 werden dann nicht die Positionen einzelner Merkmale der Fingerabdrücke, sondern die Positionsmittelwerte der aktuellen und der vorangehenden Fingerabdruckserfassung miteinander verglichen. Dies hat den Vorteil, daß statistische Abweichungen durch Dehnung oder Stauchung der Haut oder durch die Pixelrasterung der Auflagefläche 5 des Fingerabdrucksensors herausgemittelt werden, so daß der Toleranzbereich kleiner, beispielsweise zu 10 μm bis 20 μm , gewählt werden kann. Die Wahrscheinlichkeit von unberechtigten Ablehnungen der Identifikation nimmt dadurch ab.

Die Erfindung liefert ein verbessertes Verfahren zur biometrischen Benutzeridentifikation, bei dem ein Mißbrauch aufgrund von auf der Erfassungseinrichtung zurückbleibenden Fingerabdrucksspuren eines vorangehenden Benutzeridentifikationsvorgangs vermieden werden kann. Die Erfindung ist anwendbar auf die Prüfung der Benutzungsberechtigung von Geräten wie etwa Mobiltelefonen oder zur Identifikation eines Computernutzers bei Banktransaktionen. Es sind jedoch noch weitere Anwendungen denkbar, bei denen die Identität einer Person aufgrund von biometrischen Daten wie etwa eines Fingerabdrucks zuverlässig festgestellt werden muß.

Patentansprüche

1. Verfahren zur biometrischen Benutzeridentifikation, aufweisend die Schritte

5

(1) Erfassung eines biometrischen Datensatzes des Benutzers und der jeweiligen räumlichen Position der biometrischen Daten relativ zu einer Referenzposition,

10 (2) Speicherung des biometrischen Datensatzes und der zugehörigen Positionsdaten,

(3) Auslesen des biometrischen Datensatzes und der zugehörigen Positionsdaten eines dem aktuellen Benutzeridentifikationsvorgang vorangehenden Benutzeridentifikationsvorgangs,

15 (4) Vergleich der aktuell erfaßten biometrischen Daten und zugehörigen Positionsdaten mit den ausgelesenen vorhergehenden biometrischen Daten und zugehörigen Positionsdaten und Ablehnung der Identifikation dann, wenn die biometrischen Daten ein festgelegtes Maß an Übereinstimmung aufweisen und die Position der übereinstimmenden biometrischen Daten innerhalb
20 eines festgelegten Toleranzbereiches übereinstimmt.

2. Verfahren nach Anspruch 1,

d a d u r c h g e k e n n z e i c h n e t ,

25 daß der Toleranzbereich unter 100 μm , vorzugsweise bei etwa 50 μm liegt.

3. Verfahren nach Anspruch 1,

d a d u r c h g e k e n n z e i c h n e t ,

30 daß jeweils ein Mittelwert der Positionen mehrerer Einzelmerkmale der biometrischen Daten ermittelt wird und in Schritt (4) die Position der so gebildeten Mittelwerte zweier aufeinander folgender Identifikationsvorgänge verglichen werden.

35 4. Verfahren nach Anspruch 3,

d a d u r c h g e k e n n z e i c h n e t ,

daß der Toleranzbereich unter 50 μm , vorzugsweise zwischen 10 μm und 20 μm liegt.

5. Verfahren nach einem der Ansprüche 1 bis 4,
5 d a d u r c h g e k e n n z e i c h n e t ,
daß die biometrischen Daten Fingerabdrucksdaten sind.

6. Verfahren nach Anspruch 5,
d a d u r c h g e k e n n z e i c h n e t ,
10 d a ß a l s P o s i t i o n s d a t e n d i e K o o r d i n a t e n v o n G a b e l u n g e n o d e r
Minuskeln des Fingerabdrucks auf einer Auflagefläche ermit-
telt werden.

7. Verfahren nach einem der Ansprüche 1 bis 6,
15 d a d u r c h g e k e n n z e i c h n e t ,
daß nach Beendigung eines Identifikationsvorgangs die gespei-
cherten Daten des vorangehenden Identifikationsvorgangs ge-
löscht und durch die Daten des aktuellen Identifikationsvor-
gangs überschrieben werden.

20

8. Vorrichtung zur biometrischen Benutzeridentifikation, auf-
weisend
eine Einrichtung (1) zur Erfassung eines biometrischen Daten-
satzes des Benutzers und der jeweiligen räumlichen Positionen
der Daten relativ zu einer Referenzposition,
einen Speicher (3) zur Speicherung der biometrischen Daten
und der zugehörigen Positionsdaten,
eine Vergleichseinrichtung (4) zum Vergleich der biometri-
schen Daten und der zugehörigen Positionsdaten eines aktuel-
30 len Identifikationsvorgangs mit den biometrischen Daten und
zugehörigen Positionsdaten eines jeweils vorangehenden Iden-
tifikationsvorgangs, und zur Ablehnung der Identifikation,
wenn die verglichenen biometrischen Daten ein festgelegtes
Maß an Übereinstimmung aufweisen und die Positionen der über-
35 einstimmenden biometrischen Daten innerhalb eines festgeleg-
ten Toleranzbereiches übereinstimmen.

10

9. Vorrichtung nach Anspruch 8,
g e k e n n z e i c h n e t d u r c h
eine Ausgabeeinrichtung (6) zur Ausgabe des Ergebnisses der
Benutzeridentifikation.

5

10. Vorrichtung nach Anspruch 8 oder 9,
d a d u r c h g e k e n n z e i c h n e t ,
daß der Toleranzbereich unter 100 μm , vorzugsweise bei etwa
50 μm liegt.

10

11. Vorrichtung nach einem der Ansprüche 8 bis 10,
g e k e n n z e i c h n e t d u r c h
eine Einrichtung (5) zur Berechnung eines Mittelwertes der
Positionen mehrerer Einzelmerkmale der biometrischen Daten,
15 und wobei die Vergleichseinrichtung (4) die Positionen der
Mittelwerte übereinstimmender Merkmale aufeinanderfolgender
Benutzeridentifikationsvorgänge vergleicht.

20

12. Vorrichtung nach Anspruch 11,
d a d u r c h g e k e n n z e i c h n e t ,
daß der Toleranzbereich unterhalb 50 μm , vorzugsweise zwi-
schen 10 μm und 20 μm liegt.

25

13. Vorrichtung nach einem der Ansprüche 8 bis 12,
g e k e n n z e i c h n e t d u r c h
einen Fingerabdrucksensor (1) zur Erfassung des Fingerab-
drucks als biometrische Daten und dessen Position auf einem
Auflagefeld (5) des Fingerabdrucksensors (1).

30

14. Vorrichtung nach Anspruch 13,
d a d u r c h g e k e n n z e i c h n e t ,
daß der Fingerabdrucksensor (1) die Koordinaten von bestimm-
ten Merkmalen des Fingerabdrucks auf dem Auflagefeld (5) er-
mittelt.

35

15. Vorrichtung nach Anspruch 14,
d a d u r c h g e k e n n z e i c h n e t ,

11

daß die Merkmale des Fingerabdrucks Verzweigungen oder Minuskeln sind.

16. Verwendung des Verfahrens nach einem der Ansprüche 1 bis
5 7 oder der Vorrichtung nach einem der Ansprüche 8 bis 15 zur
Prüfung der Zugangsberechtigung zur Benutzung eines Mobiltelefon
oder Zugang zu einem Computernetz.

10

Zusammenfassung

Benutzeridentifikationsverfahren

5 Ein Verfahren zur biometrischen Benutzeridentifikation weist die folgenden Schritte auf:

- 10 (1) Erfassung eines biometrischen Datensatzes des Benutzers und der jeweiligen räumlichen Position der biometrischen Daten relativ zu einer Referenzposition,
- (2) Speicherung des biometrischen Datensatzes und der zugehörigen Positionsdaten,
- (3) Auslesen des biometrischen Datensatzes und der zugehörigen Positionsdaten eines dem aktuellen Benutzeridentifikationsvorgangs vorangehenden Benutzeridentifikationsvorgangs,
- 15 (4) Vergleich der aktuell erfaßten biometrischen Daten und zugehörigen Positionsdaten mit den ausgelesenen vorhergehenden biometrischen Daten und zugehörigen Positionsdaten und Ablehnung der Identifikation dann, wenn die biometrischen Daten ein festgelegtes Maß an Übereinstimmung aufweisen und die
- 20 Position der übereinstimmenden biometrischen Daten innerhalb eines festgelegten Toleranzbereiches übereinstimmt. Bei den biometrischen Daten handelt es sich vorzugsweise um Fingerabdrucksdaten.

25

(Fig. 2)

Fig. 1

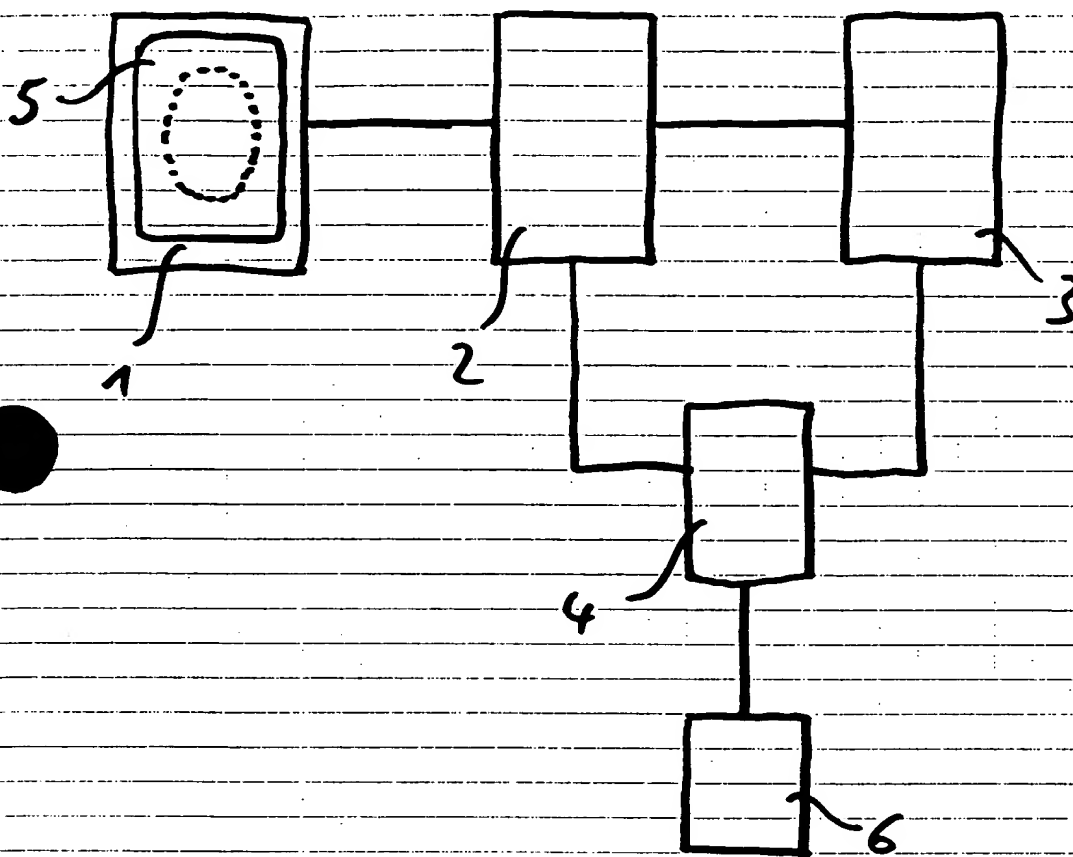


Fig. 2

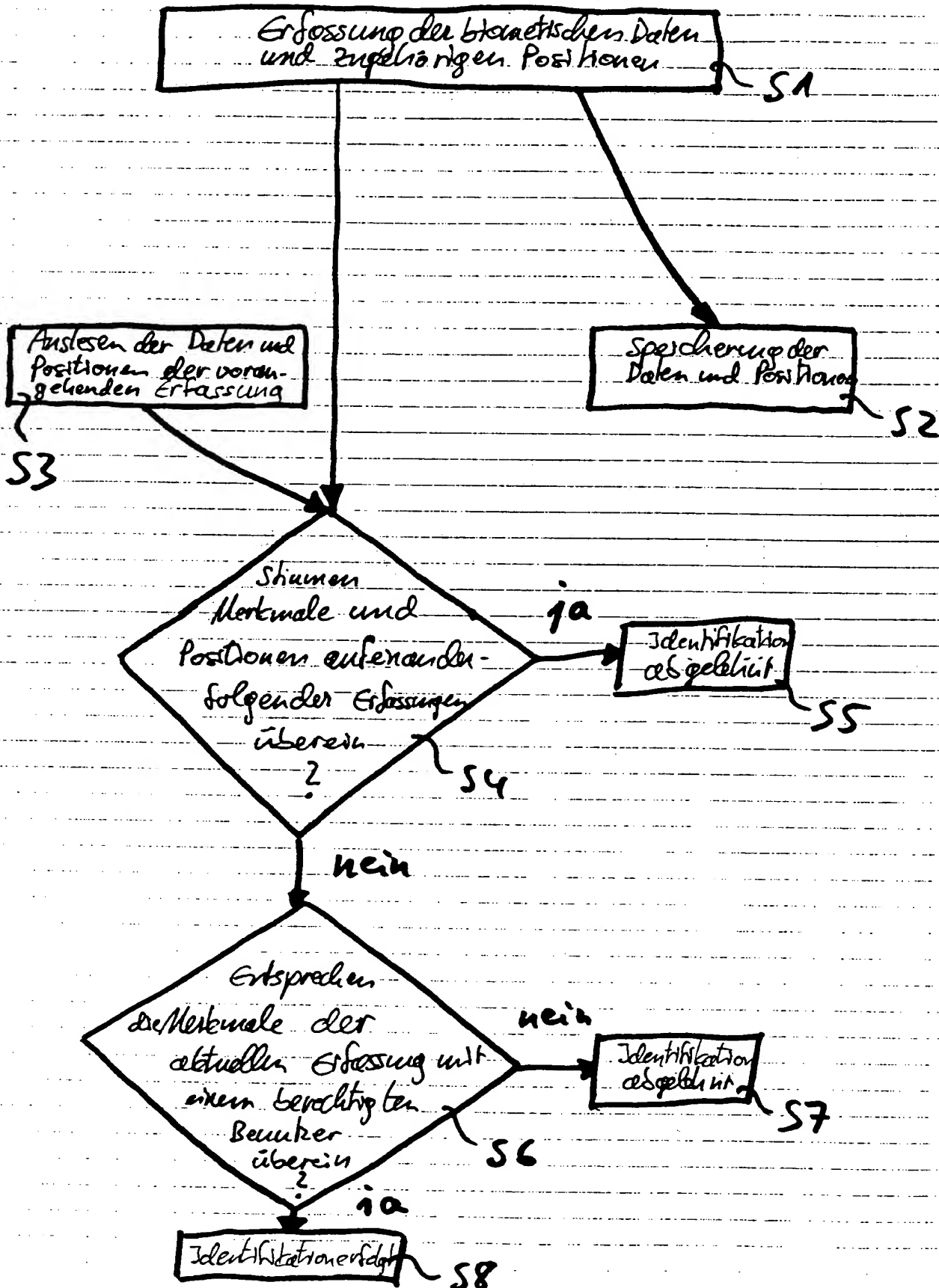
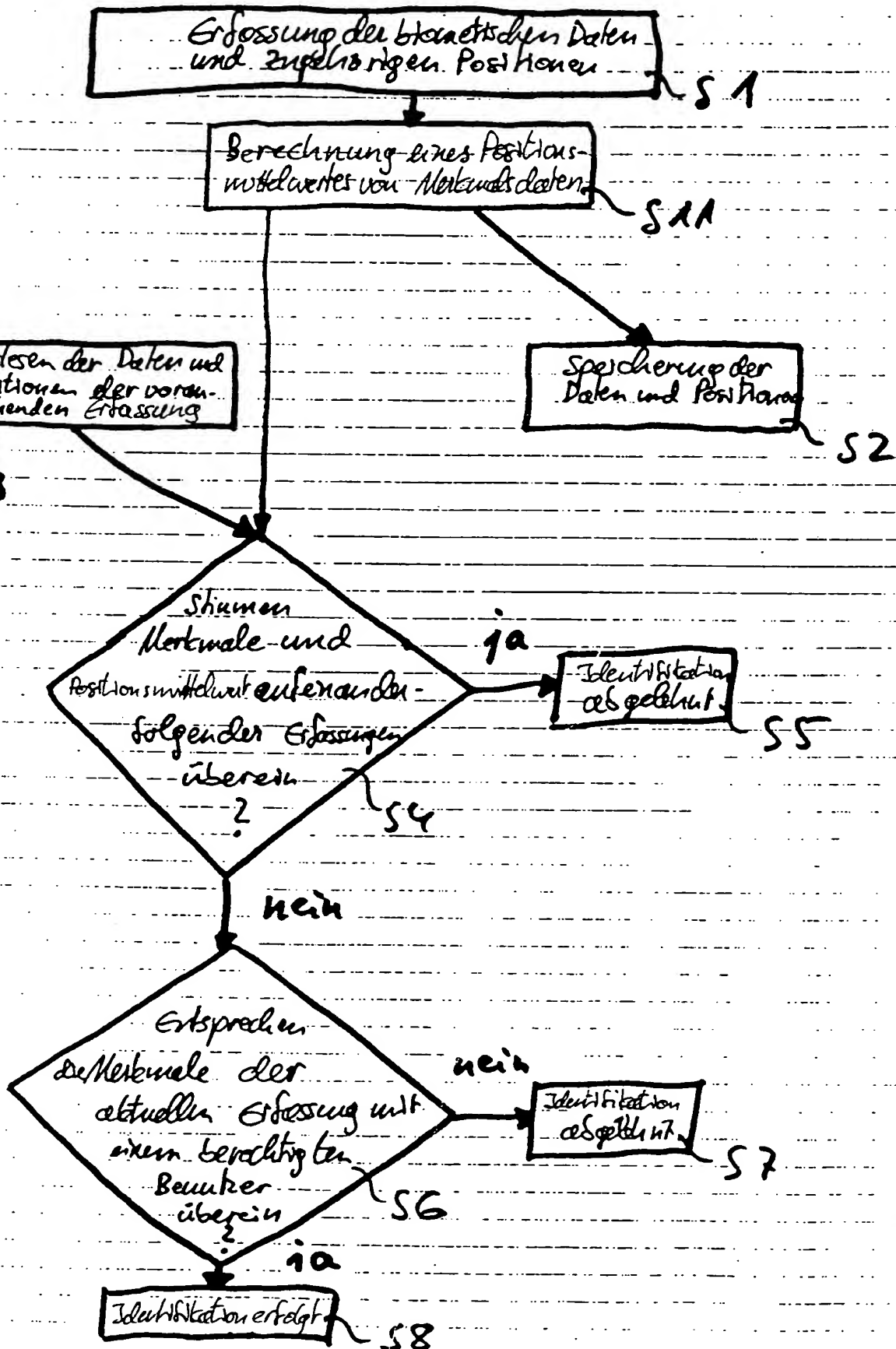


Fig. 3



This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☒ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)